



QUALYS SECURITY CONFERENCE 2018

Web Applications & APIs

The Soft Belly of the Cloud

Dave Ferguson

Director, Product Management, WAS

Remi Le Mer

Director, Product Management, WAF

Agenda

Web Apps & APIs in the Cloud

Qualys Web Application Scanning (WAS)

- Review

- What's New

- Roadmap

Qualys Web Application Firewall (WAF)

- Review

- What's New

- Roadmap

Q&A

Insecure Apps & APIs are a Problem

Your business depends on web applications

Any app or API can be a foothold into your organization

Developers are not incentivized for security

Cloud-based apps are easy for developers to deploy

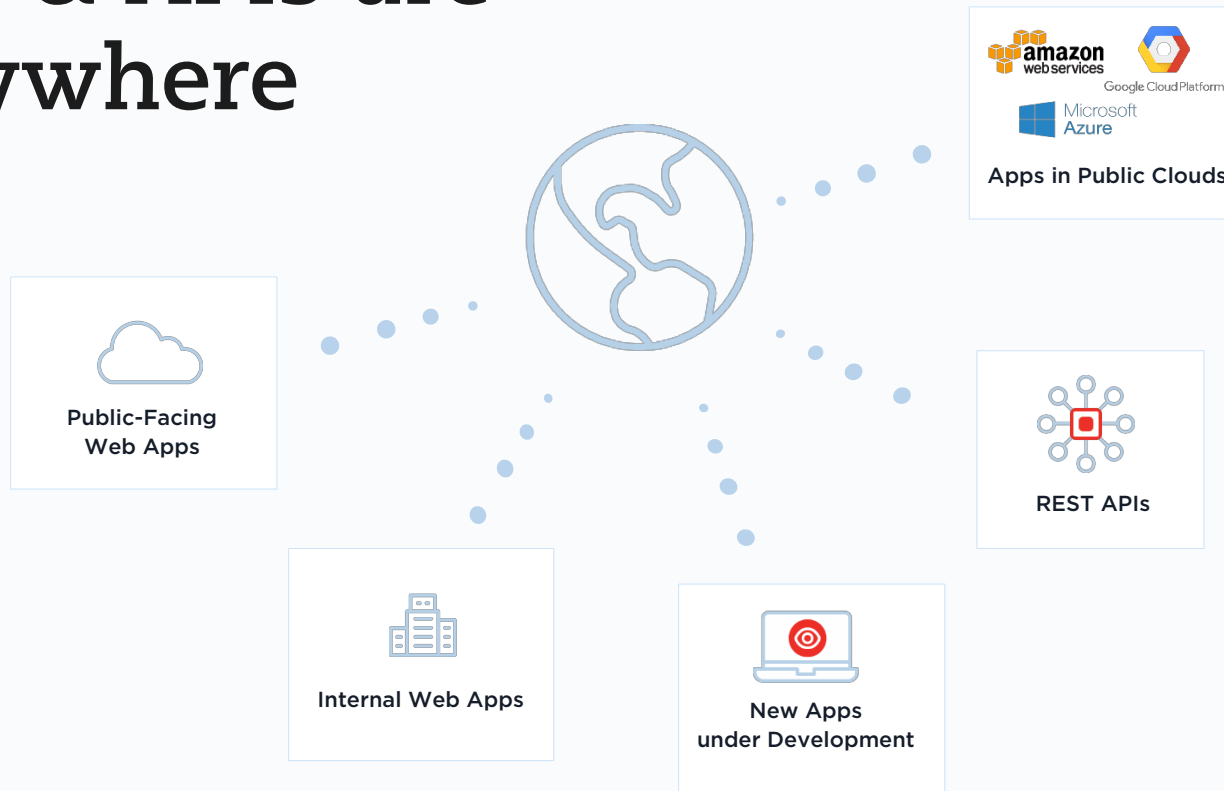
Web Applications are Being Targeted

- Most common data breach pattern *
- Top hacking vector *

U.S. Postal Service (API).....	2018
Facebook (API).....	2018
Google+ (API).....	2018
MyFitnessPal (API?).....	2017
Equifax.....	2017
Yahoo	2016
Ashley Madison.....	2015

* Source: 2018 Verizon DBIR

Apps & APIs are Everywhere



Web Application Scanning

Review

Qualys Web Application Scanning

A leading dynamic application security testing (DAST) tool

Delivered via the Qualys Cloud Platform

Identifies app-layer vulnerabilities

OWASP Top 10

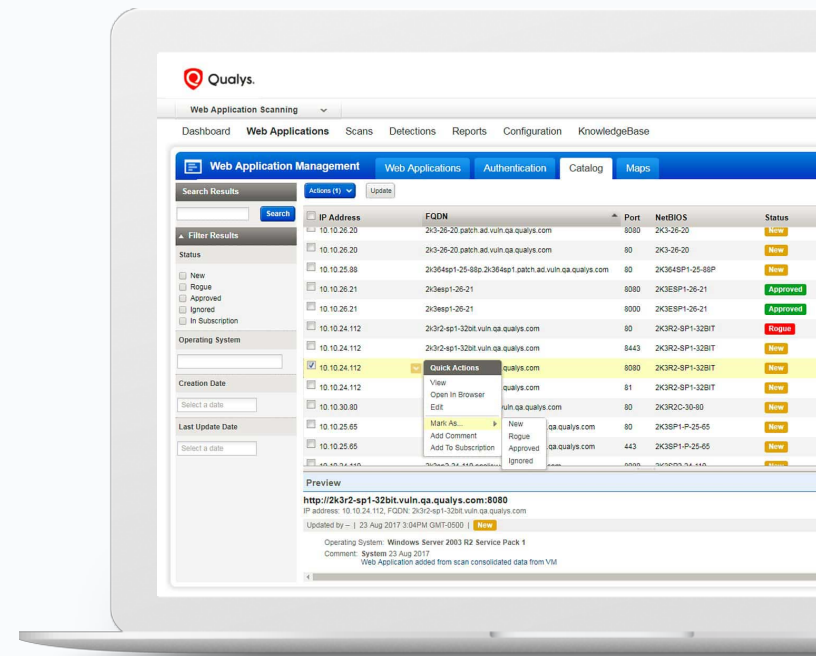
CWEs

Web-related CVEs

Includes automated crawling

Supports Selenium scripts

Malware monitoring as a bonus



Built for the Enterprise



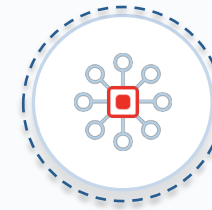
Web App Discovery
Unlimited scans &
users
RBAC
Tagging



Scheduled scans
Ad-hoc, targeted
scans
Multi-site scans
Retest vulnerability
Scan for malware



Massive scalability
Detection history
Scheduled reports
Customizable
reports
Swagger support



Robust API
CI/CD integration
Unique integration
w/Qualys WAF
Integration with
manual pen testing
tools

What's New in Qualys WAS

Scanning REST APIs



[https://
swagger.io](https://swagger.io)



[https://
www.openapis.org](https://www.openapis.org)

Swagger is specification that describes a set of REST APIs

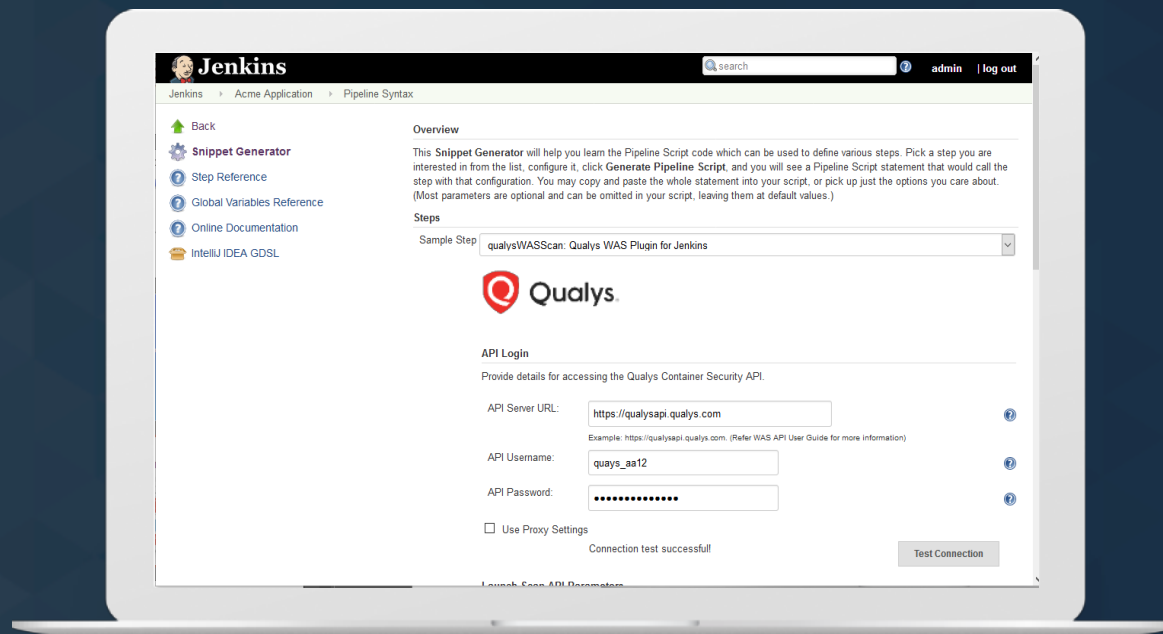
Swagger file typically available from dev team

Set Swagger file as target URL in Qualys WAS

API endpoints are automatically tested for vulnerabilities

Swagger v2 JSON format currently supported

Jenkins Plugin for WAS



Manual Testing Complements WAS

Dynamic application testing is one piece of the AppSec puzzle

Manual penetration testing important for your business-critical apps

Qualys WAS offers:

- Bugcrowd integration

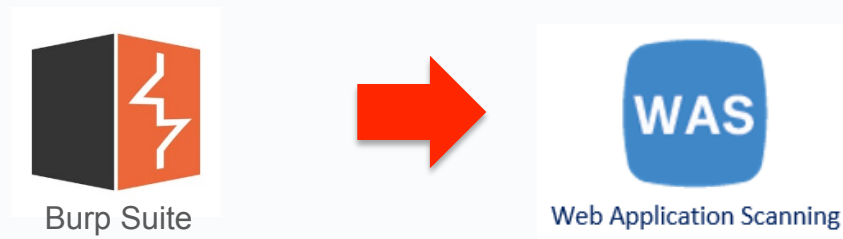
- Burp Suite integration

- Partnerships with consulting shops

Bi-directional Integration with Bugcrowd



Qualys WAS Burp Extension

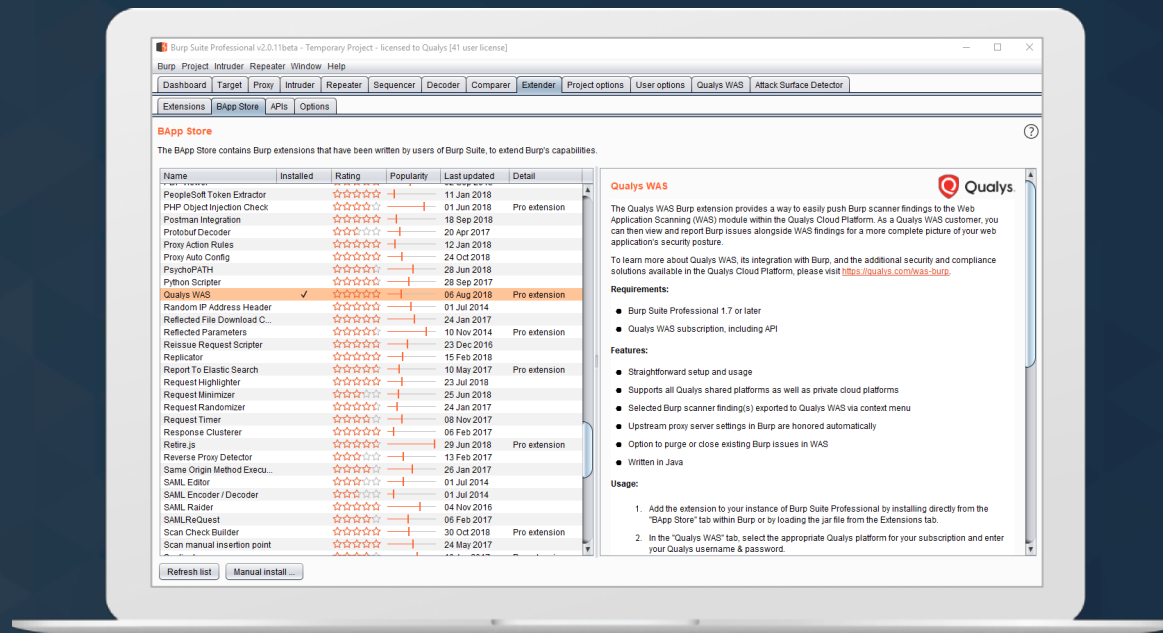


A quick, intuitive way to send Burp-discovered issues into WAS

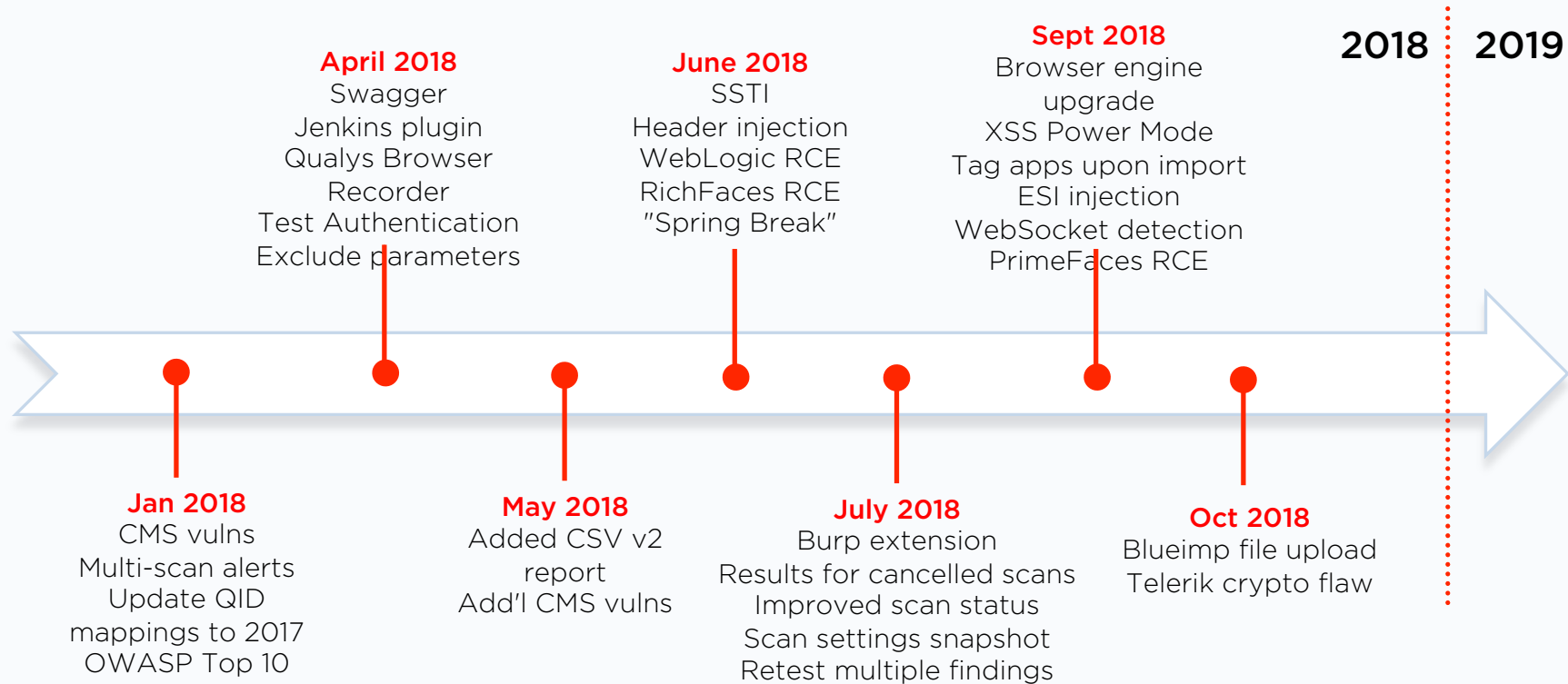
Provides centralized viewing/reporting of WAS detections + Burp issues

Available in Burp's BApp Store

Qualys WAS Burp extension

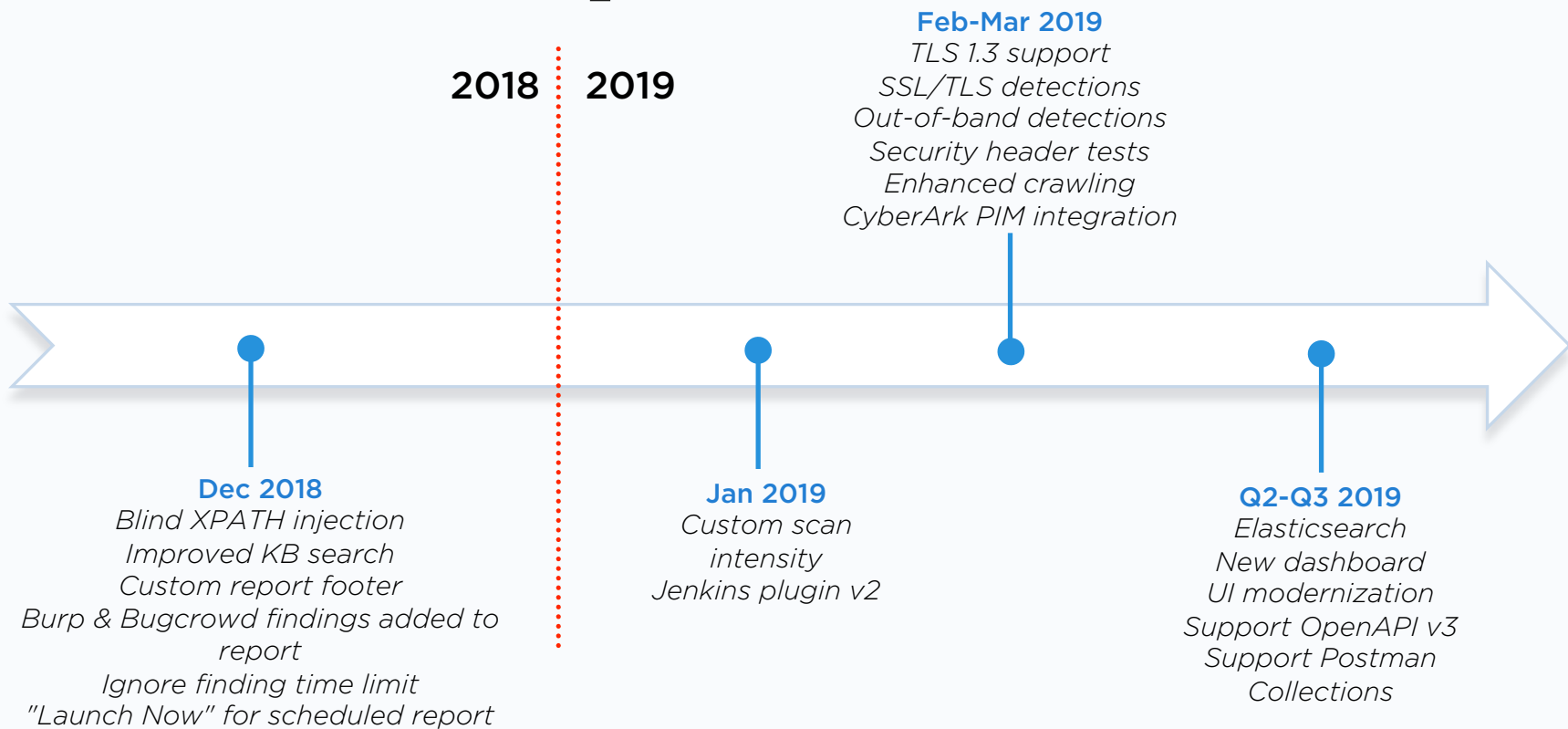


WAS Enhancements, YTD

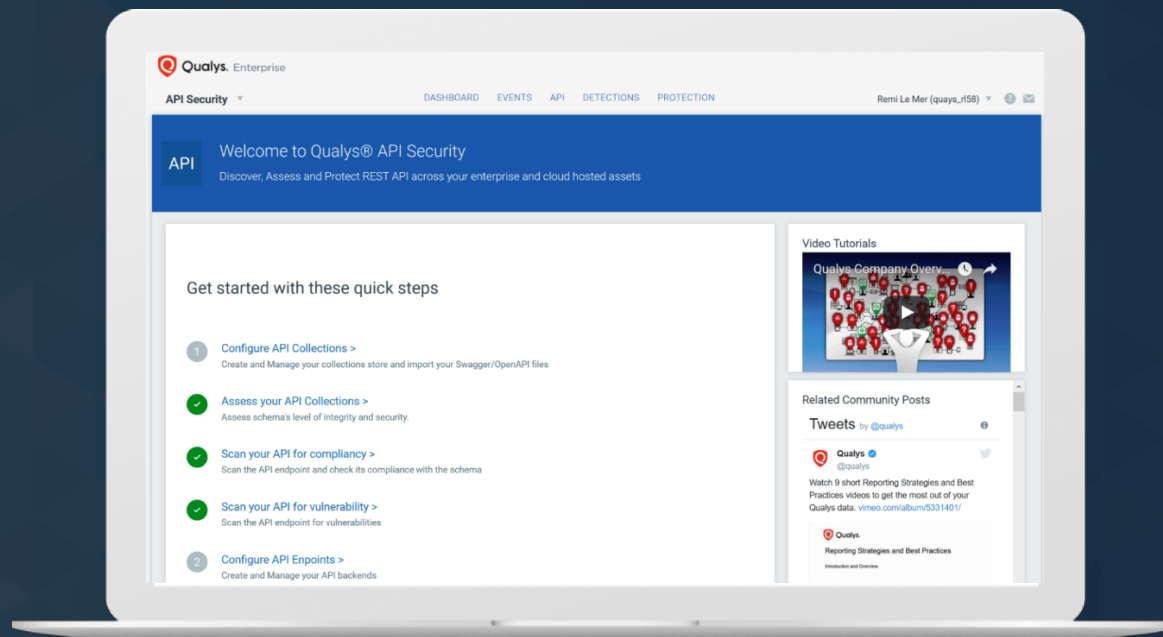


Qualys WAS Roadmap

WAS Roadmap



And Coming in 2019



Web Application Firewall

Review

Qualys WAF

Integration with WAS
Architecture improvements
Integration with Docker
Security Improvements
Roadmap – standalone
Roadmap – Integrated Suite



WAS / WAF Integration: ScanTrust

ScanTrust : Challenge your WAF protection

Assess both the application and the policy that protects it

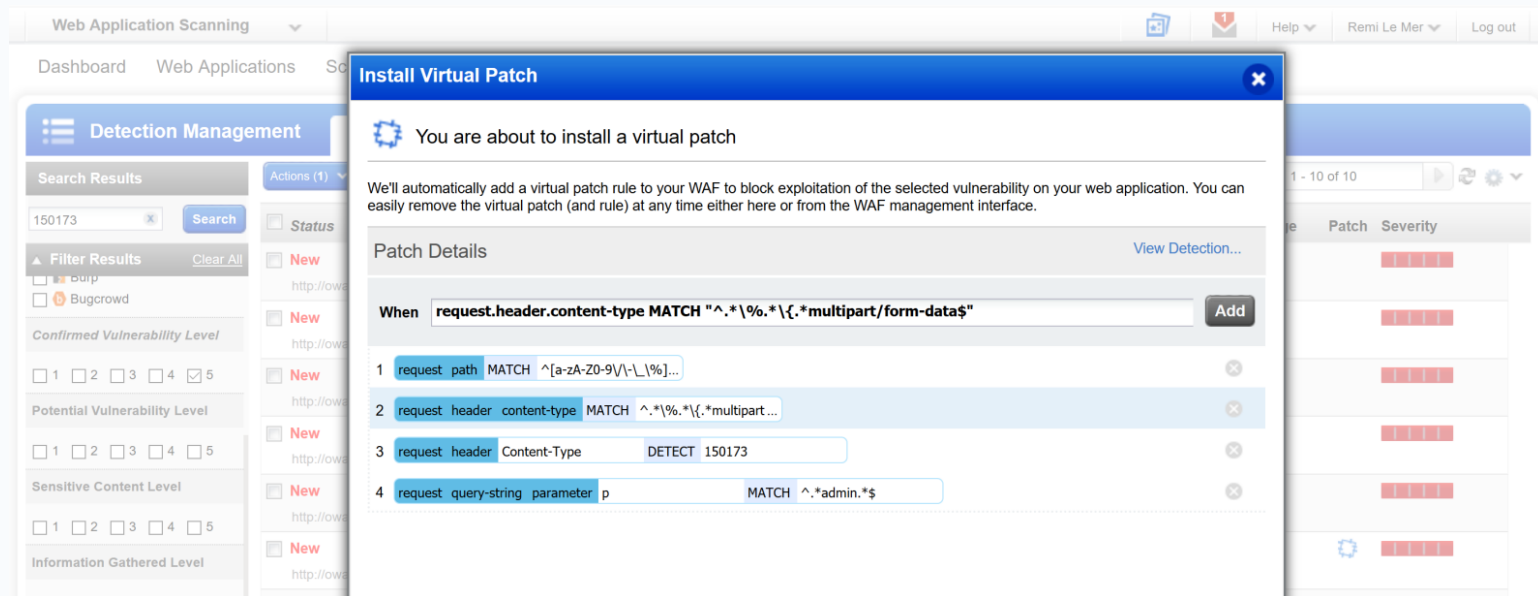
The screenshot displays the ScanTrust Detection Management interface. The top navigation bar includes 'Detection Management', 'Detection List', 'Burp', and 'Bugcrowd'. The left sidebar contains filters for 'Search Results' (with a search bar and 'Search' button), 'Filter Results' (with 'Clear All'), and various vulnerability levels (Confirmed, Potential, Sensitive Content, Information Gathered) and status (New, Active, Re-Opened, Protected, Fixed). The main table lists vulnerabilities with columns: Status, QID, Name, Group, Last Detected, Age, Patch, and Severity. The table shows several entries, including 'Blind SQL Injection' (Protected, SQL group) and 'Reflected Cross-Site Scripting (XSS) Vulnerabilities' (Protected, XSS group). A 'New' entry for 'Reflected Cross-Site Scripting (XSS) Vulnerabilities' is highlighted in yellow, with a 'Quick Actions' dropdown menu open, showing options like 'View', 'Ignore', 'Activate', 'Install Patch', 'Remove Patch', 'Edit Severity', 'Restore Standard Severity', and 'External References'.

Status	QID	Name	Group	Last Detected	Age	Patch	Severity
Protected	150012	Blind SQL Injection http://waf-demo.qualys.com/bodgeit/login.jsp	SQL	21 Sep 2017	20		High
Protected	150012	Blind SQL Injection http://waf-demo.qualys.com/bodgeit/login.jsp	SQL	21 Sep 2017	20		High
Protected	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities http://waf-demo.qualys.com/bodgeit/search.jsp	XSS	21 Sep 2017	20		High
Protected	150013	Browser-Specific Cross-Site Scripting Vulnerabilities http://waf-demo.qualys.com/bodgeit/search.jsp	XSS	21 Sep 2017	20		High
Fixed	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities http://waf-demo.qualys.com/search.jsp	XSS	27 Oct 2016	512		High
New	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities http://waf-demo.qualys.com/search.jsp	XSS		716		High

WAS / WAF Integration: Virtual Patch

Virtual Patch : One-click mitigation tool for CISO teams

Run from within WAS to address confirmed threats



December 11, 2018

What's New in Qualys WAF

Supported Platforms

Shared and Private
Qualys Cloud Platforms

Add New WAF Appliance

Select Virtual Appliance Image

Choose the virtualization platform you want to use to run your WAF appliance on.

Platform	Details
<input checked="" type="radio"/> VMware Standard	VMware virtualization platform
<input type="radio"/> Hyper-V	Microsoft Hyper-V 5.1 virtualization platform
<input type="radio"/> Amazon EC2	Amazon EC2-Classical, Amazon EC2-VPC
<input type="radio"/> Microsoft Azure	Microsoft Azure platform
<input type="radio"/> Google Cloud	Google Cloud platform
<input type="radio"/> Docker	Docker platform

CancelPreviousContinue

WAF Architecture Improvements

Easy and Usable Architecture

Virtual Reverse-Proxy

Cluster-able within hybrid topologies

Load-Balancing capabilities

SSL/TLS cipher suite categories



WAF Architecture Improvements

Virtual Appliance & Container (v1.5.3)

XML/JSON content inspection

Docker Host integration for backend automation

Better performance

Scheduled upgrades

Orchestration via Qualys API

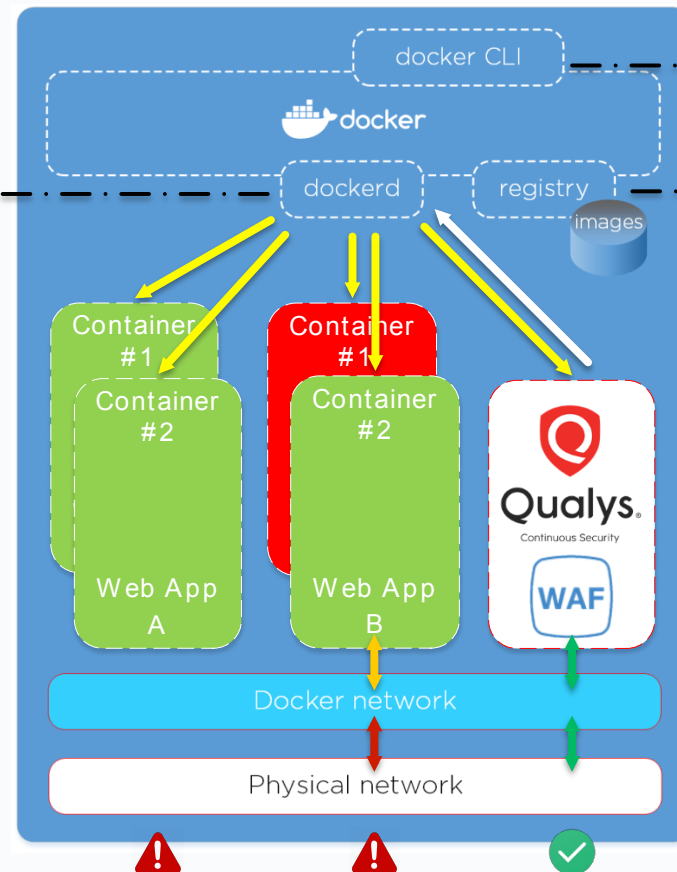


Docker

Single Host

Controls :

- containers (start | stop | delete | inspect)
- networks
- images (pull | push | delete)



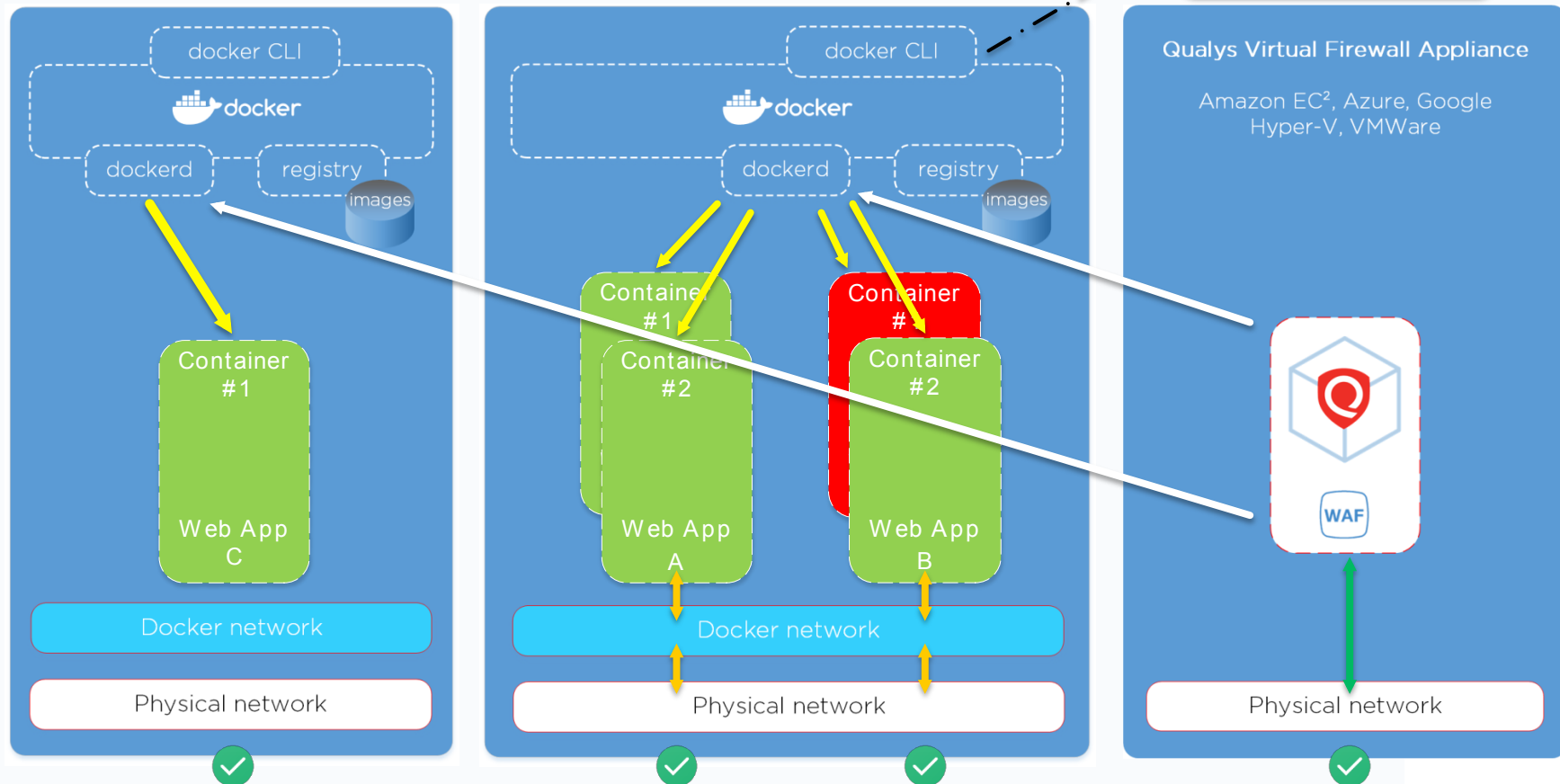
Access to docker services
via unix sockets

Stores images

Docker

Multiple Hosts

Access to docker services via network sockets



Security Improvements

Custom Rules: write and manage your own filters

- XML/JSON inspection

- Virtual Patches and Event Exceptions

- Latency control

- Rewriting capabilities (headers)

Qualys Rulesets and Templates

- DAG based inspection, programmable logic

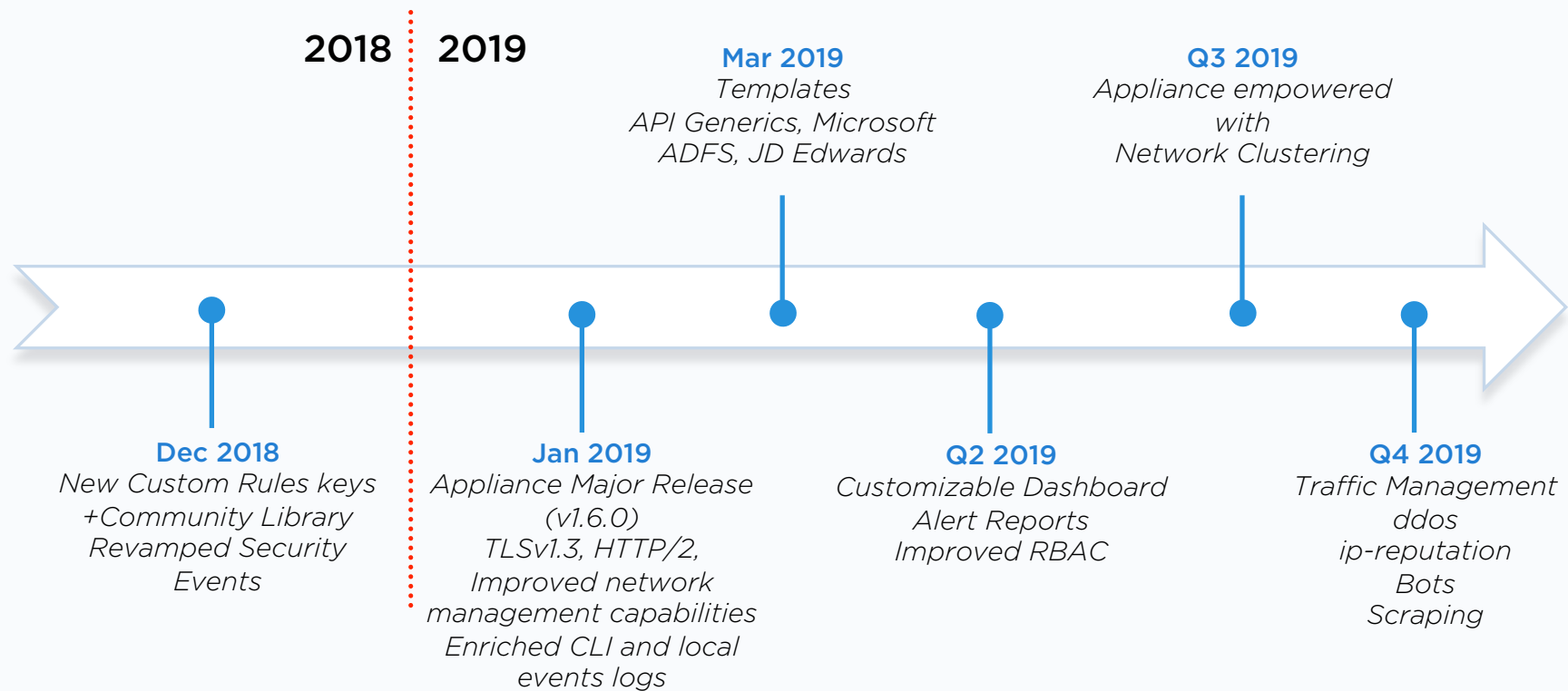
- Drupal 8.0.x, Joomla 3.4.x, Magento 2.5-2.6, Wordpress 4.2.x-4.3.x

- JBoss 4.x-7.x, OWA 2010-2017, Sharepoint 2010-2017, Tomcat 8.0.x

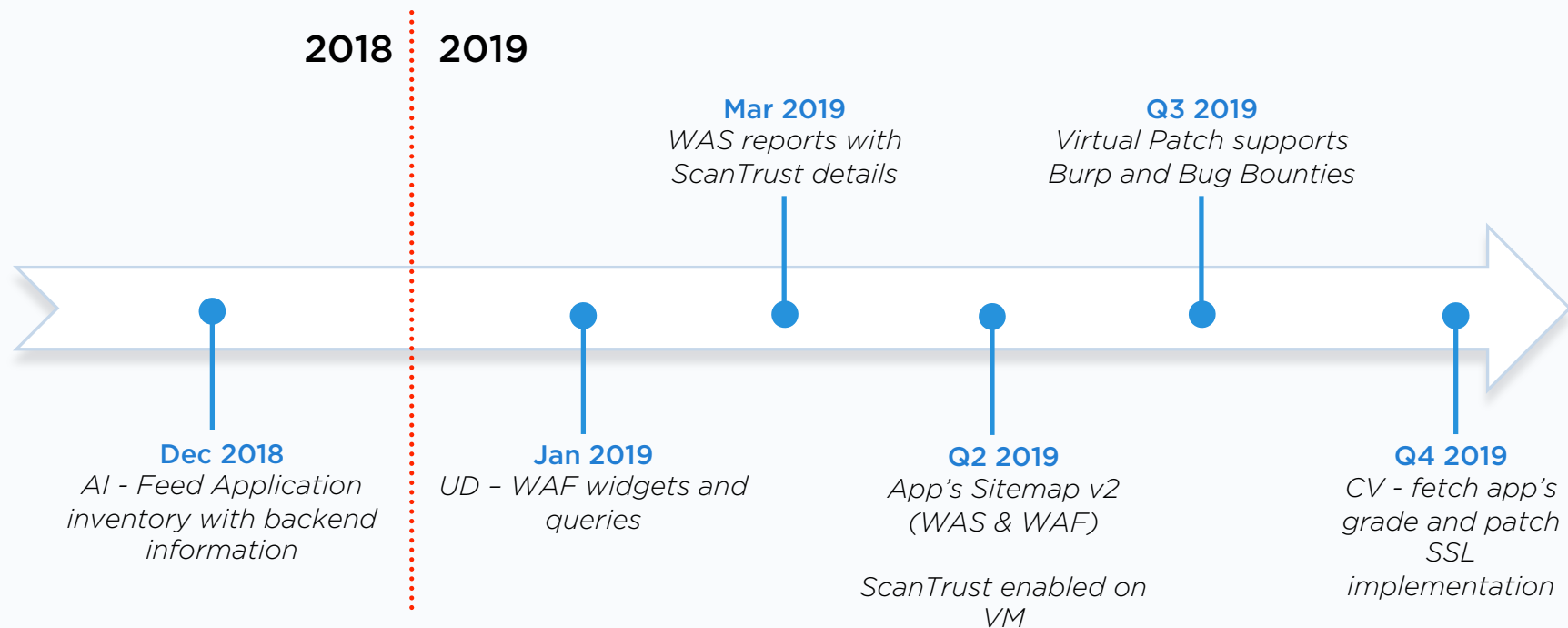
- Qualys Generics for unknown apps

Qualys WAF Roadmap

WAF Roadmap - Standalone



WAF Roadmap – Integrated Suite





QUALYS SECURITY CONFERENCE 2018

Thank You

Dave Ferguson - dferguson@qualys.com

Remi Le Mer - rlemer@qualys.com